CS458 ASSIGNMENT 2

Ching Chuen Chia

20755359

1.

a.

(i) D001 with sensitivity level B: Contact can read it but not write to it.

Contact dominates sensitivity level B

(ii) D002 with sensitivity level S: Contact can write to it but not read it

Contact is dominated by sensitivity level S

Therefore, Level S dominates Level B.

b.

(i) D276: (Unclassified, {5, 8, 13, 21})

Read Access Only

(ii) D380: (Director, {5, 13})

No Access

(iii) D340: (Customer Support, {8})

Read access Only

(iv) D425: (Management, {5, 17})

No access

(v) D118: (Consultant, {5})

Read Access Only

(vi) D644: (Management, {5, 8, 13, 21, 23, 27})

Write Access Only

c.

An application proxy can be used to block sensitive files.

d.

Step 1: write to D401 to bring down the level of sensitivity of D401 to Management.
Step 2: read a document (D118) with level of sensitivity of Consultant to reduce the contact's sensitivity level to Consultant.
Step 3: write to D401 to bring down the level of sensitivity of D401 to Consultant.
Step 4: read document (D340) with level of sensitivity of Customer Support.
Step 5: write to D401 to bring down the level of sensitivity of D401 to Customer Support.
Step 6: read document (D276) with level of sensitivity of unclassified.
Step 7: write to D401 to bring down the level of sensitivity of D401 to Customer Support to unclassified.

2.

a. It could be using SHA1 hash as SHA1 hash will produce a hash length of 40 which is the length of the hash length given. It could not be using MD5 hash as the length of the hash given is 40 and MD5 has 32 output.

b. We could utilize a rainbow table that has the precomputed hash of common guessable password and check with the hash obtained.

c. The purpose of a salt is to make sure that precomputed tables of hashes, also known as rainbow tables, will not be useful in the case of password cracking as adding a randomly generated salt will make sure that all the hashes comes out differently even if the password that was used to generate the hash is the same.
The consequence of this bug now allows the attacker to easily compute a rainbow table and use it to check it against the password hashes, allowing easier cracking of every password and that same password will have the same hash reducing the timing of cracking those password.

d. If it is non-iterative, the computation time for a hash rainbow table is very fast, which would reduce security.

3.

a. Packet Filtering Firewall

b. The firewall is situated from the outside, and blocks remote access from unauthorized IP, which means it does not block IP that is originating from inside their network.

c. Signature based anti-virus that will detect anti-virus based on a database of signature of viruses.

d. Encrypt part of the virus, or add additional useless data or lines into the virus program and recompile it.

Programming

1.

a.

Username: nvolodin
Password:
Confirmation hash value: cafebabe
Password Hash: aaaac026885224e85c4d0256ad9fb888de40e3ee

b. User: sengler

Password: bluejays

c. Input string: bob' –

iii)usually, in different programming language they have a statement where you can only insert strings or data in it that doesn't change the definition of the sql statement. For example, in java, there exists preparedstatement to prevent SQL injection.

d.

2. c. Same Origin policy will not fully prevent an XSS attack as it only prevents attackers from running scripts that are from another link, in this case, the script is fully injected into the server and will not prevent it.

   d. attribute escape before inserting untrusted data. Using html encoding to change various special character to encoded values so that the data will not be run.

3. c. use reauthentication whenever the user wants to post something.

   d. Using a CSRF token, this token will be a randomly generated hash that will prevent forms for being submitted if the hash is wrong.

   e. No. the posted data will be encrypted after the form is submitted and not before.

   f. Yes. it will work as same-origin policy is not enabled, which will allow external request to run